UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

ELVIRA VEKSLER,
Plaintiff,

-v-

WIPRO, LLC,
Defendant.

22-CV-6118 (JPO)

OPINION AND ORDER

J. PAUL OETKEN, District Judge:

Plaintiff Elvira Veksler brings this action against Defendant Wipro, LLC ("Wipro") based on Wipro's allegedly improper access to her personal computer. Veksler asserts claims under the Electronic Communications Privacy Act (ECPA), the Stored Communications Act (SCA), and the Computer Fraud and Abuse Act (CFAA), along with several state-law claims. Before the Court is Wipro's motion for summary judgment on all claims. For the reasons that follow, the motion is granted.

I. Background

The following facts are drawn primarily from the parties' Local Rule 56.1 statements and responses. (ECF Nos. 62 ("DSOF"), 70 ("PSOF").)[1]

[1] The purpose of Rule 56.1 is to assist the parties and the Court by "narrowing the scope of issues to be decided in a motion for summary judgment and by identifying the facts material and admissible to that decision-making process." *Johnson v. City of New York*, No. 15-CV-6915, 2019 WL 294796, at *10 n.8 (S.D.N.Y. Jan. 23, 2019). Accordingly, it requires that each statement or counterstatement of fact "must be followed by citation to evidence." S.D.N.Y. Loc. R. 56.1(d). Veksler's counterstatement here, however, merely denies or rephrases disputed facts from Wipro's statement, without providing any citations or evidentiary support. In the interest of deciding issues fully on the merits, the Court accepts Veksler's disputes as valid in this case, but cautions counsel in the future to follow the Court's rules more carefully. Veksler also declines to supplement her counterstatement with any additional facts material to her case. Again, in the interests of deciding issues on the merits, the Court looks instead to Veksler's declarations where necessary. (*See* ECF Nos. 68 and 71.)

Veksler was employed as a "freelance copy writer for Wipro from approximately July 16, 2021 through November 21, 2021." (DSOF ¶ 1.) While working at Wipro, Veksler was paid by an independent "recruiting and consulting services company" called Creative Circle (*id.* ¶ 2), used her own computer for her work, and worked remotely (*id.* ¶ 3). On February 10, 2022, several months after she stopped working for Wipro, Veksler emailed Francesca Nicita, a Wipro employee, stating that she was unable to "access her computer." (*Id.* ¶ 5.) After investigating Veksler's issue, "Wipro . . . determined that JAMF, Wipro's security management tool, was installed on Plaintiff's computer." (*Id.* ¶ 6.) Veksler alleges that "Wipro, without [her] knowledge or consent," installed the program "and then falsely denied that it had done so." (PSOF ¶ 6.) Wipro does not explain how the program ended up on Veksler's computer in its statement of facts, but does allege that Nicita emailed another Wipro employee stating that "Wipro never touched her laptop – never downloaded any programs." (DSOF ¶ 8.)

The parties differ on how JAMF ended up on Veksler's computer. Veksler maintains that she never authorized Wipro to install JAMF on her computer. (ECF No. 68-3 at 129:15-130:19.) Veksler's expert, Trony Clifton, opined that "[u]pon onboarding, . . . a WiPro system JAMF policy was pushed to [Veksler's] laptop." (ECF No. 63-6 ("Clifton Rep.") at 2.) Wipro's expert, FTI Consulting ("FTI"), traced the installation of JAMF to the "download of an Apple software package" on October 13, 2021—months after Veksler's onboarding. (ECF No. 63-10 ("FTI Rep.") at 4.) FTI made this determination based on a forensic examination of Veksler's computer in 2023.[2] (*Id.*) FTI concluded that "[i]t is unclear based on the artifacts examined what may have triggered JAMF to be installed," but also noted that "[f]rom our experience with Apple computers, when an install of an application is initiated, a user will be met with a pop up

[2] Clifton did not conduct such an examination. (DSOF ¶ 21; PSOF ¶ 21.)

that will require user credentials needed to authorize changes to the respective computer." (*Id.* at 5.) Wipro claims that Veksler must have consented to the installation, because the installation process requires user consent. (*See* ECF No. 64 ("Mem.") at 19-20; ECF No. 63-5 at 15:17-16:4.)

Veksler takes issue not just with JAMF, but with follow-on software she alleges was installed once JAMF was on her computer. According to Clifton, "[s]upplemental software [was] installed in addition to the JAMF software," including "CrowdStrike Falcon Sensor" ("CrowdStrike"), "a security monitoring application to detect any unauthorized intrusion." (ECF No. 63-6 at 5 (capitalization altered).) While CrowdStrike "would not disable or block [] Veksler from accessing her [computer]," it was capable of "monitoring the services that [were] being performed by the [computer]." (*Id.*) FTI found that CrowdStrike was installed shortly after the installation of JAMF on October 13, 2021. (FTI Rep. at 5.) Wipro does not deny that CrowdStrike was installed on Veksler's computer, nor does it provide an explanation for how it became installed. However, Rajiv Pillai, Chief Information Officer of Wipro, stated in his deposition that once JAMF is installed on a machine, Wipro "can install CrowdStrike, from the back end," without the computer owner's involvement. (ECF No. 63-5 at 25:2-7.)

Following Veksler's email to Nicita, Wipro contends that it spent the next six days "determining how to remove JAMF from Plaintiff's laptop as Plaintiff's ADID (Wipro credentials) were deactivated and without remotely wiping Plaintiff's laptop as there were internal concerns of possible risk of data leakage." (DSOF ¶ 9.) Veksler states that "Wipro failed to take any steps to remove JAMF and other surveillance software from Plaintiff's laptop" between February 10 and February 16, 2022. (PSOF ¶ 9.) The parties agree that Wipro removed JAMF from Veksler's computer on February 16, 2022. (DSOF ¶ 10; PSOF ¶ 10.) Veksler claims that she missed days of work and potential job interviews due to her inability to access her computer, lost files, and "suffered serious emotional and psychological harm as a result of what she perceived to be a serious invasion of her privacy." (ECF No. 69 ("Opp.") at 7.)

Veksler initiated this action on July 18, 2022. (ECF No. 1.) The operative complaint was filed on May 22, 2023. (ECF No. 39 ("SAC").) Wipro answered on November 7, 2022. (ECF No. 17.) After completing discovery, Wipro filed a motion for summary judgment on March 20, 2024. (ECF No. 61.) Veksler opposed the motion on April 17, 2024 (Opp.), and Wipro replied on April 24, 2024 (ECF No. 72 ("Reply")).

II. Legal Standard

Summary judgment is appropriate when "there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). A fact is material if it "might affect the outcome of the suit under the governing law." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). A dispute is genuine if, considering the record as a whole, a rational trier of fact could find in favor of the non-moving party. *Ricci v. DeStefano*, 557 U.S. 557, 586 (2009). The Court must "resolve all ambiguities and draw all permissible inferences in favor of the [non-movant]." *Friend v. Gasparino*, 61 F.4th 77, 84 (2d Cir. 2023) (quotation marks omitted). However, "the burden on the moving party may be discharged by 'showing'—that is, pointing out to the district court—that there is an absence of evidence to support the nonmoving party's case." *Celotex Corp. v. Catrett*, 477 U.S. 317, 325 (1986).

III. Discussion

A. Federal Claims

Veksler asserts six causes of action against Wipro. Pursuant to federal law, she asserts violations of the ECPA, 18 U.S.C. §§ 2510-11, the SCA, 18 U.S.C. § 2707, and the CFAA, 18

U.S.C. § 1030. Pursuant to New York common law, she asserts claims for negligence, trespass to chattels, and breach of the duty of good faith and fair dealing.

The Court first addresses Veksler's federal claims. All three of the federal statutes on which Veksler relies—the ECPA, the SCA, and the CFAA—prohibit only intentional conduct. The ECPA creates a cause of action against any person who "*intentionally* intercepts" (or attempts to intercept) a "wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a) (emphasis added). The SCA prohibits "*intentionally* access[ing] without authorization a facility through which an electronic communication service is provided; or . . . *intentionally* exceed[ing] an authorization to access that facility." *Id.* § 2701(a) (emphasis added).[3] Similarly, the CFAA prohibits: "knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, *intentionally* caus[ing] damage . . . ," *Id.* § 1030(a)(5)(A) (emphasis added); "*intentionally* access[ing] a protected computer without authorization, and as a result of such conduct, recklessly caus[ing] damage," *Id.* § 1030(a)(5)(B) (emphasis added); "*intentionally* access[ing] a protected computer without authorization, and as a result of such conduct, caus[ing] damage and loss," *Id.* § 1030(a)(5)(C) (emphasis added); "*intentionally* access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer," *Id.* § 1030(a)(2)(C) (emphasis added).

"Intentionally" is not defined in the ECPA, but has been interpreted by courts to be "narrower than the dictionary definition," and to require that "conduct or the causing of the result must have been the person's conscious objective." *Butera & Andrews v. Int'l Bus. Machs. Corp.*, 456 F. Supp. 2d 104, 109 (D.D.C. 2006) (quoting S. Rep. No. 99-541, at 23 (1986), *as*

[3] Veksler's second amended complaint locates her SCA claim in 18 U.S.C. § 2707 (SAC ¶ 36), but that section merely provides for a right of action for "any violation of this chapter." The only relevant violations appear in 18 U.S.C. § 2701.

reprinted in 1986 U.S.C.C.A.N. 3555, 3577) (emphasis omitted); *see also United States v. Townsend*, 987 F.2d 927, 929 (2d Cir. 1993) (explaining that "intentionally" in the context of 18 U.S.C. § 2511(1)(a) is a "synonym[] of the term 'purposefully'" and suggesting the use of jury instructions that define an intentional act as "the product of defendant's conscious objective rather than the product of a mistake or an accident"). As Veksler acknowledges, the SCA was enacted as part of the ECPA. (SAC ¶ 36.) This means that "[t]he requirement of 'intentional' conduct found in Sections 2701 and 2707 of the [SCA] was *also* enacted as part of the [ECPA]." *Butera & Andrews*, 456 F.Supp.2d at 110. Courts have accordingly interpreted it as having the same meaning as it does in the ECPA. *Id.* While the CFAA was not enacted as part of the ECPA, "similar statements regarding the definition of 'intentional' were made in connection with [its] passage," and courts have therefore defined intent in the CFAA in the same way. *Id.* Plaintiff provides no definition of intent for any of the statutes, nor does she argue why a different definition from the one proposed above would be more accurate.

While Veksler alleges that Wipro acted intentionally, Wipro contends that Veksler "has not proffered any evidence supporting this allegation because she cannot," and that "[a]ll the evidence leads to one conclusion: Plaintiff voluntarily installed JAMF onto her computer." (Mem. at 18.) In support, Wipro presents an array of evidence. It cites expert testimony (FTI Rep. at 5) and Apple documentation (ECF Nos. 63-3 at 9; 63-4 at 5-7) establishing that Veksler would have had to take some voluntary action to install JAMF. Wipro also cites internal emails expressing confusion about how the installation occurred and attempting to design safeguards to prevent similar mistakes in the future (ECF No. 63-2 at 17, 22-23, 35-36), and sworn testimony from Wipro's Chief Information Officer that only Veksler could install JAMF on her own computer (ECF No. 63-5 at 14:15-16:16). Wipro also provides the only explanation for how

CrowdStrike ended up on Veksler's computer—as follow-on software once JAMF was already installed. (ECF No. 63-5 at 25:2-7.)

In response to this, Veksler relies solely on her "unequivocal testimony that at no point did she consent to downloading JAMF." (Opp. at 12.) When asked how she knew that she had not downloaded JAMF, Veksler stated that she "was never informed of anything like JAMF," that she "would not have consented to JAMF," and that she has "enough tech skills not to do that." (ECF No. 68-3 at 130:4-19.) This constitutes at best a conclusory denial of the possibility that she accidentally downloaded JAMF. She presents no affirmative evidence that Wipro intended to install JAMF or any other program.[4] She likewise presents no evidence, nor does she even claim, that Wipro intended to cause damage, as would be required by Section (a)(2) of the CFAA. *See* 18 U.S.C. § 1030(a)(2).

Whether or not the evidence could establish that Veksler acted of her own accord, Veksler has produced no evidence beyond her own conclusory assertions that Wipro had the "conscious objective" of installing either JAMF or CrowdStrike on her computer, much less of damaging her computer or data. *Cf. Butera*, 456 F. Supp. 2d at 109. To the contrary, it appears indisputable that Wipro was initially unaware that either program had been installed, and only became aware once Veksler notified Wipro's staff. Because no rational factfinder could

[4] While Clifton's expert report states that a "Jamf [sic] policy was pushed to [Veksler's] laptop," whether or not Wipro did this intentionally is beyond the scope of the report. (Clifton Rep. at 2-3.) In addition, the "policy workflow" on which Clifton relies appears to support Wipro's account, as the workflow begins with the step "User enter username and password." (*Id.* at 3.) In any event, Clifton's account of how JAMF ended up on Veksler's computer is not credible. Clifton cites no evidence or method by which he reached his conclusions, did not conduct an examination of Veksler's computer, and opines without any justification that JAMF was installed "[u]pon onboarding" in July 2021 (Clifton Rep. at 2), when FTI's forensic examination showed that it was really installed months later (FTI Rep. at 4).

conclude that Wipro acted intentionally, Veksler's ECPA, SCA, an CFAA claims must be dismissed.

B. State Claims

In cases based on federal question jurisdiction in which "all of a plaintiff's federal-law claims are dismissed before trial, . . . a district court has discretion not to assert supplemental jurisdiction over any remaining state-law claims." *Downey v. Adloox Inc.*, No. 16-CV-1689, 2018 WL 5266875, at *9 (S.D.N.Y. Oct. 23, 2018), *aff'd*, 789 F. App'x 903 (2d Cir. 2019) (summary order). In most such cases, "'the balance of factors to be considered under the pendent jurisdiction doctrine—judicial economy, convenience, fairness, and comity—will point toward declining to exercise jurisdiction over the remaining state-law claims.'" *Id.* (quoting *Pension Benefit Guar. Corp. ex rel. St. Vincent Catholic Med. Ctrs. Ret. Plan v. Morgan Stanley Inv. Mgmt. Inc.*, 712 F.3d 705, 727 (2d Cir. 2013)).

Veksler also purports to invoke this Court's diversity jurisdiction under 28 U.S.C. § 1332. However, the Second Amended Complaint does not explicitly state an amount in controversy above $75,000 (SAC ¶ 5), nor does any previously filed complaint (*see* ECF Nos. 1 and 16). Even when pleaded expressly, conclusory allegations about the amount in controversy are "not entitled to a presumption of truth." *Wood v. Maguire Auto., LLC*, 508 F. App'x 65 (2d Cir. 2013) (summary order); *see also Suarez v. Cap. One Bank NA/FC*, No. 22-CV-568, 2022 WL 672084, at *3 (S.D.N.Y. Mar. 7, 2022) ("[W]here a complaint does not contain facts plausibly suggesting that the amount in controversy meets the jurisdictional minimum, the Court is not required to presume that the bare allegations in the complaint are a good faith representation of the actual amount in controversy."); *Weir v. Cenlar FSB*, No. 16-CV-8650, 2018 WL 3443173, at *12 (S.D.N.Y. July 17, 2018) ("The jurisdictional amount, like any other factual allegation, ought not to receive the presumption of truth unless it is supported by facts rendering it plausible.”). And, while Veksler did demand punitive damages (SAC at 15), amount-in-controversy allegations based primarily on punitive damages “are subject to ‘closer scrutiny.’” *GW Holdings Grp., LLC v. U.S. Highland, Inc.*, 794 F. App’x 49, 51 n.1 (2d Cir. 2019) (summary order) (quoting *Zahn v. Int’l Paper Co*., 469 F.2d 1033, 1033 n.1 (2d Cir. 1972)).

Here, Veksler makes no attempt whatsoever to quantify her damages. Veksler retains use of her computer to this day (DSOF ¶ 17), admits that Wipro “did not delete or remove any of [her] files” (PSOF ¶ 20),[5] does not specify any particular work that she was unable to perform or any job interviews that she missed (*cf.* Opp. at 7), and makes no effort to plead the scope of her alleged emotional damages (*id.*). The Court therefore determines that the amount-in-controversy requirement is not met, and that it lacks diversity jurisdiction.

Because Veksler’s only basis for jurisdiction is her now-dismissed federal causes of action, the Court exercises its discretion to dismiss Veksler’s remaining state-law claims without prejudice to refiling in state court.

IV. Conclusion

For the foregoing reasons, Wipro’s motion for summary judgment is GRANTED.

The Clerk of Court is directed to close the motion at ECF No. 61, enter judgment in favor of Defendant, and close this case.

SO ORDERED.

Dated: February 10, 2025
New York, New York

J. PAUL OETKEN
United States District Judge

[5] This appears to contradict Veksler’s opposition brief, which claims that “a number of files on her computer [were] permanently destroyed.” (Opp. at 7.) Per Local Rule 56.1, the Court treats Veksler’s admissions in her statement of facts as binding.